

## **Les GAFAM face aux crises migratoires: entre responsabilité numérique et solidarité internationale**

### **GAFAM and Migration Crises : Between Digital Responsibility and International Solidarity**

**Dr. ZIYANI Mehdi**

Enseignant-chercheur

Faculté des sciences juridiques et politiques

Hassan premier - Settati

Laboratoire des sciences juridiques, politiques, humaines et de la transformation numérique  
Maroc

ORCID-ID : **0009-0007-7628-5187**

**ES-SHASSAH Nawal**

Doctorante

Faculté des sciences juridiques et politiques

Hassan premier - Settati

Laboratoire des sciences juridiques, politiques, humaines et de la transformation numérique  
Maroc

ORCID-ID: **0009-0008-1977-8417**

**Dr. AKKOUR Soumaya**

Professeur d'enseignement supérieur

Faculté des sciences juridiques et politiques

Hassan premier - Settati

Laboratoire des sciences juridiques, politiques, humaines et de la transformation numérique  
Maroc

ORCID-ID : **0009-0000-3860-1440**

**Date de soumission :** 29/07/2026

**Date d'acceptation :** 22/08/2026

**Pour citer cet article :**

ZIYANI M. & al. (2026) «Les GAFAM face aux crises migratoires: entre responsabilité numérique et solidarité internationale», Revue Internationale du chercheur « Volume 7 : Numéro 3 » pp : 719-743

## Résumé

Le rôle croissant des grandes entreprises technologiques dans la gouvernance des crises migratoires soulève la question de leur contribution à la solidarité internationale et des responsabilités attachées aux fonctions qu'elles exercent. Cette étude analyse, dans une perspective juridique, institutionnelle, comparative et critique, la place des GAFAM dans les infrastructures, services et dispositifs numériques mobilisés en contexte migratoire, à partir des cadres international, européen et marocain. Elle met en évidence une contribution ambivalente : leurs capacités technologiques peuvent renforcer l'assistance, l'accès à l'information et la gestion des données, mais elles génèrent également des risques liés à la surveillance, aux discriminations, à l'opacité et à la dépendance technologique. L'étude défend ainsi une coresponsabilité humanitaire et numérique différenciée. Son apport principal réside dans la proposition d'un Cadre de coresponsabilité numérique migratoire (CRNM), structuré autour de six piliers visant à concilier innovation, primauté publique, protection des droits et redevabilité.

**Mots clés :** GAFAM ; migrations forcées ; solidarité internationale ; responsabilité numérique ; gouvernance mondiale.

## Abstract

The growing role of major technology companies in the governance of migration crises raises questions regarding their contribution to international solidarity and the responsibilities attached to the functions they perform. This study examines, from a legal, institutional, comparative and critical perspective, the role of GAFAM in the infrastructures, services and digital systems used in migration contexts, drawing on international, European and Moroccan frameworks. It highlights an ambivalent contribution: their technological capabilities may strengthen humanitarian assistance, access to information and data management, while also generating risks related to surveillance, discrimination, opacity and technological dependency. The study therefore argues for a differentiated form of humanitarian and digital co-responsibility. Its main contribution lies in proposing a Migration Digital Co-Responsibility Framework (MDCRF), structured around six pillars designed to reconcile innovation, public primacy, rights protection and accountability.

**Keywords :** GAFAM ; forced migration ; international solidarity ; digital responsibility ; global governance.

## Introduction

Les crises migratoires contemporaines constituent un défi majeur de la gouvernance mondiale. Alimentées par les conflits armés, les instabilités politiques et les catastrophes climatiques, elles mettent à l'épreuve les mécanismes classiques de solidarité internationale. Selon le Haut-Commissariat des Nations Unies pour les réfugiés (UNHCR), 117,8 millions de personnes étaient déplacées de force dans le monde à la fin de 2025<sup>1</sup>.

Ce constat invite toutefois à dépasser une lecture strictement quantitative du phénomène migratoire. Derrière l'augmentation continue des chiffres se dessine une transformation plus profonde des modalités de prise en charge des personnes déplacées. La migration forcée n'est plus seulement un fait humain, politique ou humanitaire ; elle devient également un objet de gestion informationnelle. Les parcours migratoires, les besoins de protection, les mécanismes d'assistance et même les vulnérabilités individuelles sont de plus en plus appréhendés, traduits et traités sous forme de données<sup>2</sup>. Cette évolution modifie sensiblement les termes du débat juridique : ce qui se joue désormais n'est pas uniquement la protection des personnes en déplacement, mais aussi la maîtrise des dispositifs techniques à travers lesquels cette protection est organisée<sup>3</sup>.

Dans ce contexte, les technologies numériques facilitent l'identification des personnes, les échanges d'informations et la communication entre réfugiés, autorités et organisations humanitaires. Or, une partie importante des infrastructures, services cloud, plateformes et capacités algorithmiques nécessaires à ces usages est contrôlée par de grandes entreprises technologiques, notamment les GAFAM (Google, Apple, Meta, Amazon et Microsoft). Leur puissance technique et leur influence croissante sur les processus de gouvernance<sup>4</sup> conduisent ainsi à interroger leur place dans la solidarité internationale et les responsabilités attachées aux fonctions qu'ils exercent.

Les recherches récentes ont précisément dépassé une lecture instrumentale des technologies migratoires. Elles analysent les infrastructures informationnelles hybrides, les relations public-privé et l'"appification" des frontières, en montrant que le pouvoir réside autant dans la maîtrise

---

<sup>1</sup> Haut-Commissariat des Nations Unies pour les réfugiés (UNHCR), *Global Trends 2025*, Genève, UNHCR, 2026, p. 5.

<sup>2</sup> DE MAISON ROUGE O., *Les cyberrisques : la gestion juridique des risques à l'ère immatérielle*, LexisNexis, 2018, p. 3.

<sup>3</sup> FERAL-SCHUHL C., *Cyberdroit. Le droit à l'épreuve de l'Internet*, Dalloz, éd. 2018-2019, p. 34.

<sup>4</sup> KHANAL S., ZHANG H. et TAEIHAGH A., « *Why and How Is the Power of Big Tech Increasing in the Policy Process? The Case of Generative AI* », *Policy and Society*, vol. 44, n° 1, 2025, pp. 52-69.

des données que dans la capacité à définir les catégories, les architectures d'accès et les conditions techniques de la décision publique<sup>5</sup>. D'autres travaux mettent en évidence les effets de la biométrie, de l'automatisation, de la surveillance et de la qualité imparfaite des données sur les identités migratoires, l'accès aux services et l'exercice des recours. Cette littérature demeure toutefois fragmentée : elle articule rarement, dans un même cadre normatif, la puissance fonctionnelle des GAFAM, la solidarité internationale et la répartition des responsabilités. La présente étude entend combler cette lacune en proposant un modèle permettant de traduire la responsabilité numérique en obligations institutionnelles vérifiables<sup>6</sup>.

L'idée directrice de cette recherche repose sur le constat que les GAFAM ne peuvent plus être appréhendés uniquement comme des entreprises commerciales, mais comme des acteurs globaux dont les choix technologiques et politiques ont un impact direct sur les droits fondamentaux des migrants et sur l'équilibre de la solidarité internationale. Dès lors, la problématique peut être formulée ainsi : Dans quelle mesure les géants du numérique (GAFAM) peuvent-ils être considérés comme des acteurs de la solidarité internationale face aux crises migratoires et quelle responsabilité leur incombe dans la prévention, la gestion et la réduction des vulnérabilités liées aux migrations forcées à l'ère numérique ?

L'intérêt scientifique de cette interrogation tient précisément à la zone de chevauchement qu'elle met en lumière entre plusieurs champs traditionnellement abordés séparément : le droit des migrations, le droit international, le droit du numérique, la protection des données personnelles et, plus largement, la théorie de la responsabilité. Notre réflexion s'inscrit dans cette intersection. Elle repose sur l'idée que les crises migratoires contemporaines révèlent, avec une acuité particulière, la nécessité de repenser les catégories classiques du droit lorsque la protection des personnes dépend de plus en plus d'infrastructures techniques privées et de chaînes de traitement informationnel transnationales.

---

<sup>5</sup> MEISSNER F. et TAYLOR L., « *Migration Information Infrastructures: Power, Control and Responsibility at a New Frontier of Migration Research* », *Journal of Ethnic and Migration Studies*, vol. 50, n° 9, 2024, pp. 2227-2246 ; GODIN M., OZKUL D. et HUMPHRIS R., « *Digital Technologies and Migration: Behind, Beyond and Around the Black Box* », *Journal of Ethnic and Migration Studies*, vol. 51, n° 14, 2025, pp. 3571-3589 ; MUTLU C. E., FROWD P. M. et MULLER B., « *The Appification of Borders: Data, Migration and Digitalization* », *Big Data & Society*, 2025.

<sup>6</sup> TSAGAROUSIANOU R., « *The Datafication of Migrant Bodies and the Enactment of Migrant Subjectivities* », *Media, Culture & Society*, vol. 46, n° 4, 2024 ; SEUFERLING P., « *Smart Ellis Island? Tracing Techniques of Automating Border Control* », *New Media & Society*, vol. 26, n° 9, 2024, pp. 5039-5058 ; TALAY Ö., « *How Surveillance Shapes Migrant Information Practices and Social Integration in Turkey* », *Information Development*, 2025 ; ARGYRIOU V. et LEESE M., « *Migrant Data Can Never Be Accurate* », *Journal of Ethnic and Migration Studies*, vol. 52, n° 7, 2026, pp. 1615-1633.

**Cadre théorique : des acteurs privés aux co-gouvernants fonctionnels.** La théorie de la gouvernance mondiale permet d'appréhender des acteurs privés qui, sans disposer des compétences souveraines des États, exercent une autorité fonctionnelle par l'expertise, l'infrastructure ou le contrôle de ressources indispensables. Dans le champ migratoire, les GAFAM peuvent ainsi être envisagés comme des co-gouvernants fonctionnels lorsque leurs choix d'architecture, d'hébergement ou de modération conditionnent matériellement l'accès à l'information ou à l'assistance, sans que cette qualification réduise les obligations des États<sup>7</sup>.

Cette lecture est complétée par la théorie des parties prenantes et celle des intermédiaires de régulation, qui permettent respectivement d'intégrer les populations affectées dans la gouvernance des dispositifs et d'analyser la fonction des plateformes et fournisseurs cloud dans la traduction technique des objectifs publics<sup>8</sup>. Sur cette base, la coresponsabilité numérique est conçue comme une responsabilité différenciée dont l'intensité varie selon quatre critères : le contrôle fonctionnel exercé, la capacité de prévenir le dommage, le bénéfice retiré de l'intervention et la gravité du risque pour les droits fondamentaux.

Trois hypothèses structurent cette étude. La première est que les GAFAM contribuent déjà, par leurs infrastructures et leurs technologies, à la gestion des crises migratoires. La deuxième est que cette contribution demeure ambivalente, en raison des risques qu'elle comporte en matière de désinformation, de collecte massive de données et de dépendance technologique. La troisième repose sur l'hypothèse qu'une coresponsabilité humanitaire et numérique de ces acteurs peut être envisagée, sous réserve de leur intégration progressive dans les cadres normatifs internationaux. L'hypothèse centrale est ainsi que les GAFAM constituent des acteurs hybrides de la solidarité internationale, dont l'apport potentiel à la prévention et à la gestion des vulnérabilités migratoires appelle toutefois un encadrement juridique et éthique renforcé, au regard des asymétries et dépendances susceptibles d'en résulter.

La recherche adopte une approche juridique, institutionnelle, comparative et critique. Le corpus a été constitué selon quatre critères : pertinence pour les migrations forcées ou la gouvernance numérique, autorité juridique ou évaluation scientifique par les pairs, traçabilité et actualité. Il comprend les principaux instruments internationaux, européens et marocains pertinents ainsi qu'une littérature scientifique principalement publiée entre 2017 et juillet 2026, complétée par

---

<sup>7</sup> AVANT D. D., FINNEMORE M. et SELL S. K. (dir.), « Who Governs the Globe? », Cambridge University Press, 2010.

<sup>8</sup> FREEMAN R. E., « *Strategic Management: A Stakeholder Approach* », Pitman, 1984 ; ABBOTT K. W., LEVI-FAUR D. et SNIDAL D., « *Theorizing Regulatory Intermediaries: The RIT Model* », The ANNALS of the American Academy of Political and Social Science, vol. 670, n° 1, 2017, pp. 14-35.

plusieurs références théoriques antérieures nécessaires à l’ancrage conceptuel de l’étude. Les documents institutionnels ou produits par les entreprises ne sont mobilisés que pour établir l’existence d’un programme, d’un partenariat ou d’une politique déclarée.

L’analyse combine l’interprétation des obligations applicables, la comparaison des cadres international, européen et marocain et leur confrontation aux critiques de la littérature scientifique. La démarche demeure non empirique : elle ne repose ni sur des entretiens ni sur l’accès aux contrats, codes sources ou audits internes des entreprises. Ses conclusions ont donc une portée principalement conceptuelle et normative.

L’étude analyse d’abord la place des GAFAM dans la gouvernance des crises migratoires (1), avant d’examiner les conditions d’une coresponsabilité humanitaire et numérique dans le cadre d’une solidarité internationale renouvelée (2).

## **1. Les GAFAM comme acteurs incontournables face aux crises migratoires**

### **1.1. Une puissance technologique et informationnelle au service de la gouvernance migratoire**

Les GAFAM disposent d’une puissance technologique et informationnelle sans précédent, qui leur confère un rôle central dans la gestion des crises migratoires. Cette puissance se manifeste principalement à travers la collecte, le traitement et la sécurisation des données, l’élaboration d’outils numériques pour l’identification et l’assistance humanitaire, leurs partenariats avec des organisations internationales, ainsi que leur position d’intermédiaires au sein des infrastructures informationnelles qui soutiennent la gouvernance migratoire.

Le sigle GAFAM ne doit cependant pas masquer l’hétérogénéité des fonctions exercées. Google intervient principalement par la recherche, la cartographie, l’information et certains services cloud ; Meta par la communication sociale, la diffusion et la modération des contenus ; Amazon Web Services et Microsoft Azure par l’hébergement, le calcul et les services d’intelligence artificielle ; Apple par les terminaux, les systèmes d’exploitation, les magasins d’applications et les mécanismes de sécurité et de confidentialité intégrés. Leur implication humanitaire directe est inégale. L’analyse retient donc une approche par fonctions - information, communication, infrastructure, identité et intermédiation - plutôt qu’une assimilation indifférenciée des cinq entreprises.

### 1.1.1 La collecte, le traitement et la sécurisation des données migratoires

Dans le contexte migratoire, la donnée constitue une ressource stratégique. Les États, les agences onusiennes et les ONG dépendent de systèmes numériques pour recenser, identifier et suivre les populations déplacées. Certains GAFAM, notamment les fournisseurs de services cloud et de capacités de calcul, occupent une position structurante dans l'écosystème technique supportant ces traitements. Plusieurs entreprises du groupe développent ou mettent à disposition des outils mobilisables dans l'assistance humanitaire<sup>9</sup>.

Ce point mérite d'être précisé : en droit marocain, la notion même de "prestataire de services numériques" inclut explicitement les services d'informatique en nuage (cloud) et les infrastructures d'hébergement de données<sup>10</sup>. Il s'agit donc d'une catégorie juridique qui recoupe directement les fonctions exercées par une partie des GAFAM lorsqu'ils hébergent des systèmes d'information, des bases de données, ou des plateformes de services. Cette qualification éclaire la problématique : l'intervention des GAFAM dans la gestion migratoire n'est pas extérieure au droit ; elle s'inscrit dans des catégories juridiques existantes, mais dont la mobilisation doit être clarifiée en matière d'obligations, de contrôle et de responsabilité.

Cette centralisation des données, si elle permet une efficacité accrue, soulève néanmoins des enjeux de souveraineté numérique et de protection des données personnelles, car elle place les informations sensibles des populations migrantes entre les mains d'acteurs privés dont les finalités premières demeurent commerciales<sup>11</sup>.

Cette centralisation crée également une asymétrie fonctionnelle : le contrôle de l'infrastructure conditionne la disponibilité du service, la gestion des accès et la continuité de l'assistance. En situation de crise, une telle dépendance peut devenir un risque systémique.

### 1.1.2 Des outils numériques pour l'identification et l'assistance humanitaire

Les GAFAM développent également des outils directement orientés vers l'assistance humanitaire. Facebook a, par exemple, lancé des outils de « *crisis response* » tels que « *Safety Check* », permettant aux personnes en zones de crise d'informer leurs proches de leur sécurité<sup>12</sup>.

---

<sup>9</sup> Microsoft à travers : "Using AI to Help Save Lives : AI for Humanitarian Action / Refugees and Displaced Persons, 2018." Et Google à travers Google.org, *Crisis Response : Initiatives et outils de réponse aux crises*, 2016.

<sup>10</sup> Royaume du Maroc, Loi n° 05-20 relative à la cybersécurité, art. 2, al. 10.

<sup>11</sup> TAYLOR L., « *What Is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally* », *Big Data & Society*, vol. 4, n° 2, 2017, pp. 1-14.

<sup>12</sup> Facebook (Meta Platforms, Inc.), *Crisis Response (Safety Check and Crisis Response Tools)*, Inc., 2017.



De même, *Amazon Web Services* (AWS) met en avant des solutions cloud utilisées par des organisations humanitaires pour améliorer la gestion de l'information et des opérations<sup>13</sup>.

L'intelligence artificielle et la reconnaissance biométrique constituent d'autres outils utilisés pour l'identification des réfugiés et demandeurs d'asile. L'UNHCR a notamment déployé son *Biometric Identity Management System* (BIMS) afin de renforcer l'enregistrement et la vérification de l'identité des personnes relevant de sa compétence<sup>14</sup>. Bien que ces technologies améliorent la rapidité et la précision des interventions, elles suscitent des débats éthiques quant aux risques de surveillance massive et de violations du droit à la vie privée<sup>15</sup>.

### 1.1.3. Les partenariats avec les organisations internationales

Microsoft a également contribué à la transformation numérique du Family Links Network du Comité international de la Croix-Rouge (CICR), notamment à travers la mobilisation de solutions reposant sur Microsoft Azure et ses technologies cloud<sup>16</sup>. Des dispositifs de communication et d'information destinés aux migrants ont également été soutenus dans le cadre d'initiatives portées par l'Organisation internationale pour les migrations<sup>17</sup>.

Toutefois, ces partenariats soulèvent une difficulté centrale d'attribution des responsabilités<sup>18</sup>. Lorsqu'une organisation internationale conçoit un dispositif d'assistance dont l'hébergement, la disponibilité ou certaines fonctionnalités reposent sur les services d'un prestataire privé, la répartition des obligations en matière de sécurité, de continuité du service et de protection des données doit être clairement déterminée. L'enjeu ne réside donc pas seulement dans l'existence du partenariat, mais également dans son encadrement juridique et contractuel.

### 1.1.4. De l'outil à l'infrastructure : l'intermédiation numérique comme fonction de gouvernance

Au-delà de la collecte des données, de la fourniture d'outils et des partenariats institutionnels, la puissance des GAFAM tient à leur capacité de structurer les conditions techniques dans lesquelles l'information et certains services sont rendus accessibles. Les recherches récentes

---

<sup>13</sup> Amazon Web Services, *Cloud Solutions for Humanitarian Aid Organizations*, 2020.

<sup>14</sup> UNHCR, *Biometric Identity Management System (BIMS)*, 2015.

<sup>15</sup> MOLNAR P. (2020), *Technological Testing Grounds: Migration Management Experiments and Reflections from the Ground Up*, European Digital Rights (EDRI) & Refugee Law Lab.

<sup>16</sup> Microsoft, *The International Committee of the Red Cross reunifies families separated by conflicts and disasters, keeping data secure in the Microsoft Cloud*, Microsoft Customer Stories, 4 octobre 2022.

<sup>17</sup> International Organization for Migration (IOM), *Migration Initiatives 2020: Priorities and Tools/Initiatives*, 2020.

<sup>18</sup> RICBOURG-ATTAL E., La responsabilité civile des acteurs de l'Internet, du fait de la mise en ligne de contenus illicites, *Création Information Communication*, Larcier, 2014, p. 115.



consacrées aux infrastructures informationnelles migratoires montrent que la gouvernance numérique des migrations ne se situe plus uniquement au niveau de la décision administrative finale. Elle se déploie également en amont, à travers l'architecture des systèmes, les modalités de catégorisation et de circulation des données, l'accès aux infrastructures cloud, la distribution des applications et l'organisation de la visibilité de l'information. Le pouvoir exercé par les entreprises technologiques est ainsi moins souverain que fonctionnel : sans disposer d'une compétence juridique comparable à celle des États, elles peuvent conditionner matériellement l'exercice de fonctions devenues essentielles à l'action publique et humanitaire<sup>19</sup>.

Cette approche permet également de mieux appréhender l'hétérogénéité des GAFAM. Leur influence ne résulte pas d'une intervention uniforme, mais de la maîtrise de fonctions complémentaires<sup>20</sup> : recherche et cartographie, communication sociale, hébergement et calcul, systèmes d'exploitation, distribution d'applications ou services d'intelligence artificielle. Ces différentes fonctions constituent autant de points de passage numériques susceptibles d'intervenir dans l'accès à l'information, la continuité des services et la fourniture de l'assistance. La puissance technologique des GAFAM doit dès lors être appréciée non seulement à partir des outils qu'ils mettent à disposition, mais également en fonction de leur position au sein de l'écosystème informationnel dans lequel s'organise progressivement la gouvernance migratoire. Cette position fonctionnelle explique, en retour, pourquoi leur intervention ne peut être dissociée de la question de leur responsabilité numérique.

## **1.2. Une responsabilité numérique face aux vulnérabilités migratoires**

L'implication croissante des GAFAM dans la gestion des crises migratoires ne se limite pas à la fourniture d'outils technologiques. Elle soulève une responsabilité numérique qui s'exprime dans quatre dimensions complémentaires : la lutte contre la désinformation et les discours de haine ; la protection des données personnelles et de la vie privée ; la régulation éthique des algorithmes et de l'intelligence artificielle ; enfin, la maîtrise des dépendances structurelles, de la qualité des données et des voies de recours.

### **1.2.1. Lutte contre la désinformation et les discours de haine**

Les réseaux sociaux constituent des espaces privilégiés de communication pour les migrants, mais aussi des vecteurs de désinformation et de discours de haine. Des campagnes xénophobes

---

<sup>19</sup> MEISSNER F. et TAYLOR L., op. cit. ; GODIN M., OZKUL D. et HUMPHRIS R., op. cit. ; MUTLU C. E., FROWD P. M. et MULLER B., op. cit.

<sup>20</sup> Royaume du Maroc, Directive nationale de la sécurité des systèmes d'information (DNSSI), version n° 2, 2023.

exploitent les plateformes numériques pour amplifier la peur et la stigmatisation des réfugiés. Face à cela, les GAFAM ont été appelés à assumer une responsabilité accrue. Meta et YouTube ont développé des politiques et mécanismes de modération visant à limiter les contenus de haine. Toutefois, l'efficacité de ces dispositifs reste contestée, notamment en raison des limites des systèmes automatisés de détection des discours haineux et des exigences de transparence entourant les décisions de modération<sup>21</sup>.

L'enjeu, pour notre sujet, n'est pas de refaire la théorie générale de la modération, mais d'en tirer une conséquence ciblée : dans une crise migratoire, la visibilité est une ressource. Une plateforme ne se contente pas de "héberger" des messages : elle organise la circulation, hiérarchise la visibilité, accélère certaines narrations et en ralentit d'autres. Ainsi, la responsabilité des GAFAM ne se mesure pas seulement au retrait des contenus manifestement illicites, mais aussi à la capacité de garantir un minimum de transparence sur les critères de visibilité, les mécanismes de signalement et les voies de recours, afin d'éviter qu'un contenu de protection (alerte, assistance, information fiable) ne soit neutralisé par des règles trop générales ou des automatismes.

### **1.2.2. La protection des données personnelles et de la vie privée des réfugiés**

La gestion des flux migratoires implique la collecte massive de données sensibles : biométrie, données de santé, itinéraires. Or, ces informations, lorsqu'elles sont stockées ou traitées via des infrastructures cloud privées, exposent les migrants à un risque accru de surveillance, d'usurpation d'identité ou d'utilisation abusive<sup>22</sup>. Dans ce contexte, les GAFAM sont confrontés à une responsabilité particulière : garantir que les technologies qu'ils déploient respectent les droits fondamentaux, notamment le droit à la vie privée consacré par le Pacte international relatif aux droits civils et politiques<sup>23</sup>.

Dans l'ordre juridique marocain, cette exigence trouve un fondement constitutionnel et législatif dans l'article 24 de la Constitution de 2011, relatif au respect de la vie privée, ainsi que dans les dispositions de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Cette articulation rappelle que la

---

<sup>21</sup> ZHENG J., LIU X., YANG G., HAQUE M., QIAN X., RATHNASURIYA R., YANG W. et BUDHRANI G., « HateModerate: Testing Hate Speech Detectors against Content Moderation Policies », *Findings of the Association for Computational Linguistics: NAACL 2024*, 2024, pp. 2691-2710.

<sup>22</sup> MOLNAR P. (2020), *Technological Testing Grounds: Migration Management Experiments and Reflections from the Ground Up*, European Digital Rights (EDRi) & Refugee Law Lab.

<sup>23</sup> Nations Unies, Pacte international relatif aux droits civils et politiques (PIDCP), adopté le 16 décembre 1966, art. 17.

protection de la vie privée et des données ne constitue pas un simple enjeu technique de conformité, mais une garantie fondamentale mobilisable, y compris face aux effets produits par des infrastructures numériques privées dans un contexte migratoire.

Dans cette configuration, la protection de la vie privée devient une condition d'effectivité de l'assistance : une donnée humanitaire insuffisamment protégée peut se transformer en instrument de contrôle ou de surveillance<sup>24</sup>.

### **1.2.3. Les enjeux éthiques liés à l'usage de l'IA et des algorithmes**

Enfin, les GAFAM sont responsables des outils d'intelligence artificielle qu'ils développent et qui sont parfois mobilisés dans la surveillance et le contrôle des migrations. Les systèmes de reconnaissance faciale, par exemple, peuvent contribuer à l'identification, mais ils sont aussi susceptibles de renforcer des discriminations, en raison de biais dans les données d'entraînement<sup>25</sup>.

Le cadre européen n'est plus une simple proposition : le règlement (UE) 2024/1689 sur l'intelligence artificielle classe parmi les systèmes à haut risque plusieurs usages déployés par ou pour les autorités compétentes en matière de migration, d'asile et de contrôle des frontières<sup>26</sup>. Cette qualification soumet ces usages à des exigences renforcées de gestion des risques et de protection des droits fondamentaux. La Recommandation de l'UNESCO sur l'éthique de l'intelligence artificielle complète cette approche en insistant sur la responsabilité, la transparence et la prévention des atteintes aux droits humains<sup>27</sup>.

### **1.2.4. Limites structurelles, contre-arguments et conditions de légitimité**

Un premier contre-argument tient au solutionnisme technologique. L'efficacité, la rapidité ou la personnalisation annoncées ne suffisent pas à démontrer qu'un dispositif améliore la protection. L'accès inégal aux terminaux, à la connexion, à la langue ou à l'identité numérique peut transformer l'outil d'assistance en condition d'accès au droit. L'obligation d'utiliser une application ou une plateforme peut également déplacer vers le migrant la charge de prouver son

---

<sup>24</sup> MARELLI M., *"Handbook on Data Protection in Humanitarian Action"*, 3e éd., Cambridge University Press, 2024.

<sup>25</sup> BUOLAMWINI J. et GEBRU T., « *Gender Shades : Intersectional Accuracy Disparities in Commercial Gender Classification* », *Proceedings of Machine Learning Research*, vol. 81, 2018, pp. 1-15.

<sup>26</sup> U.E., Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle, JOUE L, 12 juillet 2024, notamment annexe III, point 7.

<sup>27</sup> UNESCO, Recommandation sur l'éthique de l'intelligence artificielle, UNESCO, 2021.

identité, son parcours ou sa vulnérabilité, alors même qu'il se trouve dans une situation de dépendance<sup>28</sup>.

Un deuxième contre-argument concerne l'opacité propriétaire et la dépendance contractuelle. La centralisation auprès d'un fournisseur peut créer un verrouillage technologique, limiter la portabilité des données et rendre difficile l'audit indépendant. Surtout, la donnée migratoire n'est jamais une représentation parfaitement neutre : sa qualité dépend des catégories retenues, des erreurs d'enregistrement, des changements de situation et des objectifs de l'institution qui la produit. Une décision automatisée peut ainsi consolider une approximation en apparence objective<sup>29</sup>.

Enfin, la responsabilité privée ne doit pas devenir un mécanisme de déresponsabilisation publique. Les GAFAM ne sont pas parties aux conventions relatives au statut des réfugiés et ne peuvent décider souverainement de l'accès au territoire ou à la protection. En revanche, lorsqu'un système privé contribue matériellement à une décision, l'État doit garantir l'accès à une motivation intelligible, à une révision humaine et à un recours effectif ; l'entreprise doit, pour sa part, rendre disponibles les éléments techniques nécessaires à l'audit et à la contestation. Les difficultés rencontrées par le contentieux stratégique contre les systèmes automatisés confirment la nécessité d'organiser en amont l'accès à la preuve technique<sup>30</sup>.

## **2. Vers une solidarité numérique internationale dans la gestion des crises migratoires**

### **2.1. La nécessaire coopération entre États, organisations internationales et GAFAM**

La gestion des crises migratoires dépasse largement les capacités individuelles des États. Elle appelle à une coopération renforcée entre les différents acteurs de la communauté internationale, parmi lesquels les GAFAM se sont imposés comme partenaires en raison de leur puissance technologique. Cette coopération ne peut toutefois produire une solidarité numérique durable qu'à la condition d'articuler partage des responsabilités, équité dans la répartition des charges, gouvernance sécurisée des données et institutionnalisation de mécanismes de coordination entre les différents acteurs.

---

<sup>28</sup>MORGAN H., « *Everyday Digital Dis/connection: Locating Slow Violence in (Non)encounters with the UK Asylum State* », Transactions of the Institute of British Geographers, vol. 49, n° 4, 2024, e12674 ; MUTLU C. E., FROWD P. M. et MULLER B., op. cit.

<sup>29</sup>ARGYRIOU V. et LEESE M., op. cit. ; MEISSNER F. et TAYLOR L., op. cit.

<sup>30</sup>PALMIOTTO F. et OZKUL D., « *Climbing a Wall: Strategic Litigation Against Automated Systems in Migration and Asylum* », German Law Journal, vol. 25, n° 6, 2024, pp. 935-955.

### **2.1.1. Le partage des responsabilités et la sécurisation des voies migratoires à l'ère numérique**

Les migrations forcées résultent souvent de conflits armés, de crises climatiques ou de violations massives des droits humains. Les GAFAM peuvent contribuer indirectement par des outils d'alerte, de cartographie et d'analyse informationnelle mobilisables en contexte humanitaire. Cette coopération s'inscrit dans le cadre normatif international, notamment le Pacte mondial pour des migrations sûres, ordonnées et régulières<sup>31</sup> et le Pacte mondial sur les réfugiés<sup>32</sup>. Ces instruments consacrent l'idée d'une responsabilité partagée et de la mobilisation de partenaires, y compris non étatiques.

Les outils numériques peuvent contribuer à sécuriser les parcours migratoires. Les plateformes d'information et de communication permettent aux migrants d'accéder à des informations fiables sur leurs droits, sur les procédures d'asile, et sur les voies légales de migration. Des initiatives de « *digital tools for migration management* » sont documentées par l'Organisation internationale pour les migrations<sup>33</sup>.

Dans le contexte marocain, cette dynamique trouve un écho particulier : le Maroc a adopté une Stratégie nationale d'immigration et d'asile (SNIA) en 2014 (Ministère chargé des Marocains résidant à l'étranger et des affaires de la migration, 2014).

La SNIA de 2014 permet aussi de fonder une lecture "pragmatique" : elle assume une approche humanitaire et une mise en cohérence avec les engagements internationaux, dans une logique de protection et d'intégration. Cette orientation permet de montrer que l'enjeu n'est pas seulement de "numériser" la migration, mais de construire des voies sûres et régulières appuyées sur des outils numériques fiables, tout en maintenant des garanties relatives à la qualité, à la sécurité et à la confidentialité de l'information ainsi qu'au contrôle des accès. La loi n° 05-20 fournit le socle de cybersécurité applicable aux systèmes d'information concernés, tandis que la loi n° 43-20 encadre les services de confiance pour les transactions électroniques et contribue à la sécurisation juridique des échanges numériques.

---

<sup>31</sup> Nations Unies, Pacte mondial pour des migrations sûres, ordonnées et régulières, 2018.

<sup>32</sup> Nations Unies, Pacte mondial sur les réfugiés (*Global Compact on Refugees*), 2018.

<sup>33</sup> International Organization for Migration (IOM), Migration Initiatives 2020: Priorities and Tools/Initiatives, International Organization for Migration, 2020.

### **2.1.2. Les défis liés à l'inégale répartition des charges et le rôle des GAFAM**

La coopération internationale en matière migratoire se heurte à l'inégale répartition des charges entre les États<sup>34</sup>. Les GAFAM, grâce à leurs ressources considérables, peuvent contribuer à soutenir des capacités nationales et internationales, mais cette coopération ne doit pas conduire à une substitution des acteurs privés aux institutions publiques. Le droit marocain, à travers la Constitution de 2011, réaffirme l'attachement du Royaume aux conventions internationales relatives aux droits humains et consacre des garanties fondamentales<sup>35</sup>. Cette exigence doit guider l'intégration des GAFAM dans la gouvernance migratoire, afin que leur action relève d'une complémentarité encadrée.

### **2.1.3. Gouvernance des données humanitaires : sécurité, contrôle et réversibilité**

Au-delà de la coopération politique, la solidarité numérique suppose une gouvernance des données humanitaires. Dans les crises migratoires, les flux d'informations circulent entre États, agences, ONG, plateformes et prestataires techniques : cette circulation exige une logique de chaîne de confiance, fondée sur la traçabilité des accès, la limitation des habilitations, la justification des finalités, et la documentation des traitements. Autrement dit, il ne suffit pas d'« avoir des données » ; il faut pouvoir démontrer la licéité, la proportionnalité et la sécurité des opérations, surtout lorsque les personnes concernées se trouvent en situation de vulnérabilité<sup>36</sup>.

Dans cette perspective, l'intégration des GAFAM dans les dispositifs de coopération doit être conditionnée à des garanties minimales : auditabilité des systèmes, notification d'incidents, portabilité des données et réversibilité contractuelle, afin d'éviter qu'une assistance efficace à court terme ne produise une dépendance structurelle à moyen terme. Cette exigence rejoint, dans le contexte marocain, l'idée que la sécurisation des infrastructures et la confiance dans les échanges numériques constituent un socle permettant de mieux encadrer les partenariats sans affaiblir la capacité de contrôle des acteurs publics. Cette dynamique a récemment été renforcée par le décret n° 2-24-921 du 22 octobre 2024 relatif au recours aux prestataires de services Cloud par les entités et les infrastructures d'importance vitale disposant de systèmes

---

<sup>34</sup> GUILD E., COSTELLO C., GARLICK M., MORENO-LAX V. et CARRERA S., *Enhancing the Common European Asylum System and Alternatives to Dublin*, étude réalisée pour la Commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du Parlement européen, Parlement européen, 2015.

<sup>35</sup> Royaume du Maroc, Constitution du Royaume du Maroc, 2011.

<sup>36</sup> Comité international de la Croix-Rouge (CICR), Manuel sur la protection des données dans l'action humanitaire, 3e éd., CICR, 2025.

d'information ou de données sensibles<sup>37</sup>, puis par l'arrêté du Chef du gouvernement n° 3-17-25 du 1er août 2025 fixant le référentiel des exigences de qualification de ces prestataires<sup>38</sup>. Ce dispositif renforce notamment les exigences de sécurité, de gouvernance, de répartition des responsabilités et de réversibilité applicables au recours au cloud.

#### **2.1.4. De la coopération ponctuelle à une gouvernance multi-acteurs institutionnalisée**

La coopération entre États, organisations internationales et entreprises technologiques ne saurait toutefois reposer exclusivement sur des partenariats ponctuels ou sur la mise à disposition volontaire de ressources techniques. Dès lors que des infrastructures ou services privés participent durablement à des fonctions d'information, d'assistance ou de gestion des données migratoires, leur articulation avec l'action publique doit s'inscrire dans des mécanismes institutionnels de coordination. Une gouvernance multi-acteurs suppose ainsi une définition préalable des mandats, l'identification de l'autorité publique compétente, une répartition transparente des fonctions ainsi que l'existence de procédures communes de coordination et d'évaluation. L'intégration des GAFAM ne doit donc pas conduire à leur transférer des prérogatives souveraines, mais à organiser juridiquement et institutionnellement leur contribution autour d'une primauté maintenue des autorités publiques et des organisations compétentes.

Une telle gouvernance implique également de dépasser une conception exclusivement institutionnelle du partenariat en intégrant les personnes migrantes et les organisations qui les représentent parmi les parties prenantes des dispositifs numériques. Lorsqu'une architecture technique affecte directement l'accès à l'information, à l'assistance ou à l'exercice d'un droit, les personnes concernées ne peuvent être considérées comme de simples utilisatrices du service. Leur participation à la conception, à l'évaluation et à la révision des dispositifs contribue à rapprocher la performance technique de l'effectivité des droits. Les GAFAM peuvent ainsi être intégrés à une gouvernance migratoire multi-acteurs en qualité de partenaires fonctionnels, à condition que leurs fonctions demeurent identifiables, encadrées et contrôlables. L'institutionnalisation de cette coopération constitue alors le point de passage entre la

---

<sup>37</sup> Décret n° 2-24-921 du 22 octobre 2024 relatif au recours aux prestataires de services Cloud par les entités et les infrastructures d'importance vitale disposant de systèmes d'information ou de données sensibles.

<sup>38</sup> Arrêté du Chef du gouvernement n° 3-17-25 du 7 safar 1447 (1er août 2025) fixant le référentiel des exigences de qualification des prestataires de services Cloud.



mobilisation ponctuelle des capacités technologiques et la construction d'une véritable coresponsabilité humanitaire et numérique.<sup>39</sup>

## **2.2. Pour une coresponsabilité humanitaire et numérique**

### **2.2.1. Vers une reconnaissance normative de la coresponsabilité humanitaire et numérique des GAFAM**

La responsabilité sociale des entreprises a longtemps été conçue comme volontaire. Toutefois, dans le cas des GAFAM, une approche plus exigeante se justifie. Les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme consacrent la responsabilité des entreprises de respecter les droits humains dans l'ensemble de leurs activités<sup>40</sup>. Au Maroc, cette exigence rejoint les engagements constitutionnels relatifs à la dignité et aux droits fondamentaux.

Les GAFAM sont déjà partenaires d'organisations internationales. Toutefois, une coresponsabilité suppose une reconnaissance plus explicite et des mécanismes de redevabilité. Les deux Pactes mondiaux de 2018 fournissent un cadre discursif et coopératif mobilisable pour intégrer le secteur privé, sans dissoudre la primauté des États.

### **2.2.2. Perspectives : encadrement juridique, cybersécurité et gouvernance mondiale inclusive**

La coresponsabilité ne peut se concrétiser sans points d'appui normatifs permettant d'encadrer l'intervention des acteurs technologiques. Sans consacrer directement une coresponsabilité des GAFAM en matière migratoire, le règlement (UE) 2024/1689 fournit, par son approche fondée sur les risques, une référence utile pour penser l'encadrement des systèmes d'intelligence artificielle susceptibles d'affecter les droits fondamentaux<sup>41</sup>. La Recommandation de l'UNESCO sur l'éthique de l'intelligence artificielle complète cette approche par des principes de responsabilité, de proportionnalité et de respect des droits humains<sup>42</sup>.

---

<sup>39</sup> FREEMAN R. E., op. cit. ; ABBOTT K. W., LEVI-FAUR D. et SNIDAL D., op. cit.

<sup>40</sup> Nations Unies, Principes directeurs relatifs aux entreprises et aux droits de l'homme : Mise en œuvre du cadre « Protéger, respecter et réparer », OHCHR, 2011, principe 11.

<sup>41</sup> U.E., Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle, JOUE L, 12 juillet 2024.

<sup>42</sup> UNESCO, Recommandation sur l'éthique de l'intelligence artificielle, UNESCO, 2021.

### 2.2.3. Le Cadre de coresponsabilité numérique migratoire (CRNM)

Afin de dépasser une contribution seulement descriptive, cette étude propose un Cadre de coresponsabilité numérique migratoire (CRNM). Celui-ci organise une chaîne d'obligations différenciées entre autorités publiques, organisations internationales, opérateurs humanitaires et entreprises technologiques. Il repose sur le principe suivant : plus un acteur contrôle une fonction essentielle, possède la capacité de prévenir le dommage, retire un bénéfice de l'intervention et expose les personnes à un risque élevé, plus ses obligations de prévention, de transparence et de réparation doivent être fortes.

| Pilier                                                        | Exigences minimales                                                                                                                                                                                                            | Indicateurs de mise en œuvre                                                                                                |
|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>1. Primauté publique et mandat légal</b>                   | Décision finale conservée par l'autorité compétente ; attribution contractuelle explicite des responsabilités ; interdiction de déléguer à une entreprise la détermination souveraine du statut ou de l'accès à la protection. | Mandat publié ; matrice des responsabilités ; identification de l'autorité décisionnaire ; clause de suspension du service. |
| <b>2. Finalité humanitaire, nécessité et proportionnalité</b> | Limitation des finalités ; collecte strictement nécessaire ; évaluation préalable des impacts sur les droits fondamentaux ; réexamen périodique de la nécessité du dispositif.                                                 | Registre des finalités ; analyse d'impact ; justification de chaque catégorie de données ; calendrier de révision.          |
| <b>3. Gouvernance des données et cybersécurité</b>            | Minimisation, chiffrement, contrôle des accès, journalisation, durée de conservation limitée, notification des incidents et garanties pour les transferts transfrontières.                                                     | Journaux d'accès ; plan de conservation ; rapport d'incident ; audit indépendant de sécurité ; tests de continuité.         |

| <b>Pilier</b>                                            | <b>Exigences minimales</b>                                                                                                                                                                                            | <b>Indicateurs de mise en œuvre</b>                                                                                   |
|----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>4. Intégrité algorithmique et supervision humaine</b> | Qualité des données ; tests de biais ; explicabilité adaptée au contexte ; intervention humaine réelle ; interdiction d'une décision défavorable exclusivement automatisée lorsque des droits essentiels sont en jeu. | Rapports de tests ; documentation du modèle ; taux de révision humaine ; mécanisme d'arrêt ou de contournement.       |
| <b>5. Transparence, auditabilité et recours</b>          | Information accessible ; motifs compréhensibles ; audit externe ; mécanisme de plainte ; accès à la preuve technique nécessaire à la contestation ; réparation des préjudices.                                        | Rapport public de transparence ; délais de réponse ; statistiques de recours ; suivi des mesures correctrices.        |
| <b>6. Portabilité, réversibilité et participation</b>    | Interopérabilité ; plan de sortie ; prévention du verrouillage fournisseur ; consultation des migrants, ONG et autorités de contrôle dans la conception et l'évaluation.                                              | Standards ouverts ; test de réversibilité ; plan de migration ; comité de parties prenantes ; exercices de transfert. |

Source : élaboration des auteurs.

Le CRNM doit fonctionner à trois moments : ex ante, par l'analyse d'impact, la définition du mandat et les clauses contractuelles ; pendant le déploiement, par la surveillance, les audits, la participation et la gestion des incidents ; ex post, par l'accès au recours, la réparation, la publication des résultats et, si nécessaire, le retrait du système. Sa mise en œuvre suppose une autorité de contrôle indépendante et une articulation claire entre droit des migrations, protection des données, cybersécurité, droit de la concurrence et régulation de l'intelligence artificielle.

#### **2.2.4. La redevabilité comme condition d'une solidarité numérique légitime**

Une coresponsabilité humanitaire et numérique ne peut être seulement déclarée ; elle doit être vérifiable. Cette exigence suppose de traduire les principes précédemment identifiés en obligations de transparence, de contrôle et de recours. Lorsque des entreprises technologiques

structurent des dispositifs migratoires d'enregistrement, d'assistance, d'identité ou d'accès, les logiques techniques et organisationnelles susceptibles d'affecter l'effectivité des droits doivent pouvoir être documentées et contrôlées. L'approche par les risques du règlement (UE) 2024/1689<sup>43</sup> fournit une grammaire opérationnelle : documentation, traçabilité, qualité des données, supervision humaine et contrôle renforcé des usages sensibles.

La responsabilité des entreprises, telle qu'affirmée par les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme, suppose que l'acteur privé respecte les droits humains dans l'ensemble de ses activités, y compris lorsque ses choix d'architecture (centralisation, opacité, dépendances techniques) produisent des effets prévisibles sur les personnes. Transposés au champ migratoire et au cadre proposé dans cette étude, ces principes conduisent à concevoir un devoir de vigilance fonctionnel : anticiper les risques de surveillance, de discrimination, d'indisponibilité ou de verrouillage technologique, et prévoir des mécanismes de recours et de contrôle compatibles avec la protection des personnes<sup>44</sup>.

## Conclusion

L'analyse confirme que les GAFAM sont devenus des acteurs fonctionnels de la gouvernance migratoire. Leur apport ne se limite pas à des dons ou à des partenariats ponctuels : il réside dans le contrôle d'infrastructures, de canaux d'information, de services cloud et de dispositifs algorithmiques dont dépend une partie de l'assistance humanitaire<sup>45</sup>. Cette capacité justifie leur intégration dans les cadres de responsabilité, sans leur reconnaître un pouvoir souverain.

La réponse à la problématique est donc nuancée. Les GAFAM peuvent contribuer à la solidarité internationale en renforçant la rapidité, la continuité et la portée de l'action humanitaire ; toutefois, cette contribution devient illégitime lorsqu'elle repose sur une collecte disproportionnée, une surveillance opaque, une décision non contestable ou une dépendance technologique durable<sup>46</sup>. La capacité technique ne vaut pas, à elle seule, garantie juridique.

L'apport principal de l'étude réside dans la formalisation du Cadre de coresponsabilité numérique migratoire. Celui-ci transforme une notion générale de responsabilité partagée en six piliers opérationnels et en obligations graduées selon le contrôle, la capacité, le bénéfice et

<sup>43</sup>U.E., Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle, JOUE L, 12 juillet 2024.

<sup>44</sup> Nations Unies, Principes directeurs relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre « Protéger, respecter et réparer, OHCHR, 2011, principes 11 et 17 à 22.

<sup>45</sup> MEISSNER F. et TAYLOR L., op. cit. ; GODIN M., OZKUL D. et HUMPHRIS R., op. cit. ; KHANAL S., ZHANG H. et TAEIHAGH A., op. cit.

<sup>46</sup> TAYLOR L., op. cit. ; MORGAN H., op. cit. ; PALMIOTTO F. et OZKUL D., op. cit.

le risque. Les Pactes mondiaux de 2018, le règlement (UE) 2024/1689 et la Recommandation de l'UNESCO<sup>47</sup> fournissent les points d'appui normatifs de ce modèle<sup>48</sup>.

Le cadre marocain - Constitution de 2011, loi n° 09-08, loi n° 05-20, loi n° 43-20, Stratégie nationale d'immigration et d'asile et Directive nationale de sécurité des systèmes d'information - offre des fondements pour encadrer les données, la cybersécurité<sup>49</sup> et les services de confiance<sup>50</sup>. Il gagnerait cependant à prévoir plus explicitement les partenariats technologiques humanitaires, les audits indépendants, la réversibilité des services cloud et l'accès des personnes concernées à un recours effectif.

Les limites de la recherche doivent enfin être rappelées : l'étude est doctrinale, ne mesure pas empiriquement la performance des outils et ne dispose pas des contrats ou audits internes des entreprises. Ces limites ouvrent un programme de recherche fondé sur des études de cas, des entretiens avec les organisations humanitaires et les personnes migrantes, ainsi que l'évaluation comparative de dispositifs concrets. La solidarité numérique ne sera durable que si l'innovation demeure subordonnée à la dignité, aux droits fondamentaux, à la maîtrise publique et à une redevabilité effectivement contrôlable.

---

<sup>47</sup> UNESCO, *Recommandation sur l'éthique de l'intelligence artificielle*, Paris, UNESCO, 2021

<sup>48</sup> U.E., Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle, JOUE L, 12 juillet 2024.

<sup>49</sup> Royaume du Maroc, Loi n° 05-20 relative à la cybersécurité

<sup>50</sup> Royaume du Maroc, Loi n° 43-20 relative aux services de confiance pour les transactions électroniques.

## Bibliographie :

### A. Doctrine / articles / rapports :

ABBOTT K. W., LEVI-FAUR D. & SNIDAL D. (2017). *Theorizing regulatory intermediaries: The RIT model*. The ANNALS of the American Academy of Political and Social Science, 670(1).

DOI : <https://doi.org/10.1177/0002716216688272>

ARGYRIOU V. & LEESE M. (2026). “*Migrant data can never be accurate*’: *Studying migration and borders through the notion of data quality*. Journal of Ethnic and Migration Studies, 52(7), 1615-1633.

DOI : <https://doi.org/10.1080/1369183X.2025.2600050>

AVANT D. D., FINNEMORE M. & SELL S. K. (dir.) (2010). *Who Governs the Globe?* Cambridge University Press.

DOI : <https://doi.org/10.1017/CBO9780511845369>

Amazon Web Services. *Cloud solutions for humanitarian aid organizations* (2020).  
<https://aws.amazon.com/government-education/nonprofits/>

BUOLAMWINI J., & GEBRU T., *Gender shades: Intersectional accuracy disparities in commercial gender classification*, *Proceedings of Machine Learning Research* (2018).  
<https://proceedings.mlr.press/v81/buolamwini18a.html>

DE MAISON ROUGE O., *les cyberisques, la gestion juridique des risques à l'ère immatérielle*, lexisnexis, édition 2018.

FERAL-SCHUHL C., *Cyberdroit, Le Droit à l'épreuve de l'internet*, Dalloz, édition 2018/2019.

FREEMAN R. E. (1984). *Strategic Management: A Stakeholder Approach*. Pitman.

Facebook (Meta Platforms, Inc.). *Crisis Response (Safety Check and crisis response tools)* 2017. <https://www.facebook.com/about/crisisresponse/>

GODIN M., OZKUL D. & HUMPHRIS R. (2025), *Digital technologies and migration: Behind, beyond and around the black box*. Journal of Ethnic and Migration Studies, 51(14).

DOI : <https://doi.org/10.1080/1369183X.2025.2513153>

Google.org. *Crisis Response (initiatives et outils de réponse aux crises)* 2016.  
<https://crisisresponse.google/>

GUILD E., COSTELLO C., GARLICK M., MORENO-LAX V. & CARRERA S. (2015). *Enhancing the Common European Asylum System and Alternatives to Dublin*. Study for the

European Parliament, Committee on Civil Liberties, Justice and Home Affairs (LIBE).  
European Parliament.

<https://www.rsc.ox.ac.uk/publications/enhancing-the-common-european-asylum-system-and-alternatives-to-dublin>

HUMPHRIS R., HUDSON G. & BAZURLI R. (2025), *Digital internal bordering: Surveillance, data-sharing, and the fate of sanctuary cities*. Journal of Ethnic and Migration Studies.

DOI : <https://doi.org/10.1080/1369183X.2025.2513166>

International Committee of the Red Cross. (2021). *The ICRC and data protection* (cadre et principes de protection des données). ICRC.

<https://www.icrc.org/en/icrc-and-data-protection>

International Organization for Migration. (2020). *Migration Initiatives 2020* (priorités et outils/initiatives). IOM.

[https://publications.iom.int/system/files/pdf/mi\\_2020.pdf](https://publications.iom.int/system/files/pdf/mi_2020.pdf)

KHANAL S., ZHANG H., & TAEIHAGH A., (2025). *Why and how is the power of Big Tech increasing in the policy process? The case of generative AI*. Policy and Society, 44(1).

DOI : <https://doi.org/10.1093/polsoc/puae012>

MARELLI M. (dir.) (2024), *Handbook on Data Protection in Humanitarian Action*, 3e éd., Cambridge University Press.

DOI : 10.1017/9781009414630

MEISSNER F. & TAYLOR L. (2024), *Migration information infrastructures: Power, control and responsibility at a new frontier of migration research*, Journal of Ethnic and Migration Studies, 50(9).

DOI : <https://doi.org/10.1080/1369183X.2024.2307772>

MORGAN H. (2024), *Everyday digital dis/connection: Locating slow violence in (non)encounters with the UK asylum state*. Transactions of the Institute of British Geographers, 49(4), e12674.

DOI : <https://doi.org/10.1111/tran.12674>

MUTLU C. E., FROWD P. M. & MULLER B. (2025), *The appification of borders: Data, migration and digitalization*, Big Data & Society.

DOI : <https://doi.org/10.1177/20539517251319996>



Meta Platforms, Inc. (2021). *Community Standards Enforcement Report*. Meta Transparency Center.

<https://transparency.meta.com/reports/community-standards-enforcement/>

Microsoft. (2022). The International Committee of the Red Cross reunifies families separated by conflicts and disasters, keeping data secure in the Microsoft Cloud. Microsoft Customer Stories.

<https://www.microsoft.com/en/customers/story/1550914630508022658-icrc-nonprofit-microsoft-cloud>

Microsoft. (2018). *Using AI to help save lives (AI for Humanitarian Action / refugees and displaced persons)*. Microsoft.

<https://blogs.microsoft.com/on-the-issues/2018/09/24/using-ai-to-help-save-lives/>

MOLNAR P. (2020), *Technological Testing Grounds: Migration Management Experiments and Reflections from the Ground Up*, European Digital Rights (EDRi) & Refugee Law Lab.

<https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf>

PALMIOTTO F. & OZKUL D. (2024), *Climbing a Wall: Strategic litigation against automated systems in migration and asylum*. German Law Journal.

DOI : <https://doi.org/10.1017/glj.2024.52>

RICBOURG-ATTAL E., *La responsabilité civile des acteurs de l'internet, du fait de la mise en ligne de contenus illicites*, Création Information Communication, Larcier (2014).

SEUFERLING P. (2024), *Smart Ellis Island? Tracing techniques of automating border control*, New Media & Society, 26(9), 5039-5058.

DOI : <https://doi.org/10.1177/14614448241251802>

TALAY Ö. (2025), *How surveillance shapes migrant information practices and social integration in Turkey*. Information Development.

DOI : <https://doi.org/10.1177/02666669251373044>

TSAGAROUSIANOU R. (2024), *The datafication of migrant bodies and the enactment of migrant subjectivities: Biometric data, power and resistance at the borders of Europe*, Media, Culture & Society, 46(4).

DOI : <https://doi.org/10.1177/01634437231214193>

TAYLOR L., (2017). *What is data justice? The case for connecting digital rights and freedoms globally*. Big Data & Society, 4(2).

DOI : <https://doi.org/10.1177/2053951717736335>

United Nations High Commissioner for Refugees (UNHCR). (2026). Global Trends 2025. Genève : UNHCR.

<https://www.unhcr.org/sites/default/files/2026-06/global-trends-report-2025.pdf>

United Nations High Commissioner for Refugees (UNHCR) & Accenture Development Partnerships. (2016). *Connecting refugees: How Internet and mobile connectivity can improve refugee well-being and transform humanitarian action*. UNHCR.

<https://www.unhcr.org/5770d43c4.pdf>

UNHCR. (2015). *Biometric Identity Management System (BIMS)*.

<https://www.unhcr.org/sites/default/files/legacy-pdf/550c304c9.pdf>

Ministère chargé des Marocains résidant à l'étranger et des affaires de la migration. (2014). Stratégie nationale d'immigration et d'asile (SNIA). Rabat.

[https://www.oriental.ma/wp-content/uploads/2021/01/File\\_1\\_861.pdf](https://www.oriental.ma/wp-content/uploads/2021/01/File_1_861.pdf)

ZHENG J., LIU X., YANG G., HAQUE M., QIAN X., RATHNASURIYA R., YANG W. et BUDHRANI G., « HateModerate: Testing Hate Speech Detectors against Content Moderation Policies », *Findings of the Association for Computational Linguistics: NAACL 2024*, 2024.

DOI : <https://doi.org/10.18653/v1/2024.findings-naacl.172>

## **B. Textes, conventions, protocoles et instruments normatifs**

Arrêté du Chef du gouvernement n° 3-17-25 du 7 safar 1447 (1er août 2025) fixant le référentiel des exigences de qualification des prestataires de services Cloud.

Comité international de la Croix-Rouge (CICR). (2025). Manuel sur la protection des données dans l'action humanitaire, 3e éd. CICR.

Décret n° 2-24-921 du 22 octobre 2024 relatif au recours aux prestataires de services Cloud par les entités et les infrastructures d'importance vitale disposant de systèmes d'information ou de données sensibles

Directive nationale de la sécurité des systèmes d'information, version n°2, 2023.

[Directive nationale de la sécurité des systèmes d'information \(DNSSI\) | DGSSI](#)

Nations Unies (1966). Pacte international relatif aux droits civils et politiques (PIDCP).  
<https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

Nations Unies (2011). Principes directeurs relatifs aux entreprises et aux droits de l'homme : Mise en œuvre du cadre "Protéger, respecter et réparer". OHCHR.

[https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr\\_en.pdf](https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf)

Nations Unies (2018a). Pacte mondial pour des migrations sûres, ordonnées et régulières.

[https://refugeesmigrants.un.org/sites/default/files/180711\\_final\\_draft\\_0.pdf](https://refugeesmigrants.un.org/sites/default/files/180711_final_draft_0.pdf)

Nations Unies (2018b). Pacte mondial sur les réfugiés (*Global Compact on Refugees*).

<https://globalcompactrefugees.org/sites/default/files/2019/12/Global%20compact%20on%20refugees%20EN.pdf>

Royaume du Maroc (2011). *Constitution du Royaume du Maroc*.

<https://www.chambrederespresentants.ma/fr/la-constitution-du-royaume-du-maroc-2011>

Royaume du Maroc (2020). Loi n° 05-20 relative à la cybersécurité. DGSSI.

<https://www.dgssi.gov.ma/sites/default/files/legislative/brochure/2023-03/loi%2005-20.pdf>

Royaume du Maroc (2021). Loi n° 43-20 relative aux services de confiance pour les transactions électroniques. DGSSI.

<https://www.dgssi.gov.ma/sites/default/files/legislative/brochure/2023-03/loi%2043-20.pdf>

Royaume du Maroc. Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, promulguée par le dahir n° 1-09-15 du 18 février 2009, Bulletin officiel n° 5714 du 5 mars 2009.

U.E. (2024). Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (règlement sur l'intelligence artificielle). Journal officiel de l'Union européenne, L, 12 juillet 2024.

<https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=fr>

UNESCO. (2021). Recommandation sur l'éthique de l'intelligence artificielle.

<https://unesdoc.unesco.org/ark:/48223/pf0000380455>